State of North Carolina

Information Resource Management Commission

Statewide Security Assessment Project Agency Preparation Communications Package

Version No. PV1

September 24, 2003

Table of Contents

1.0 Purpose

Pursuant to North Carolina Session Law 2003-153, the State Chief Information Officer is charged with performing security assessments of all Executive Branch agencies. In response to this new Session Law, the Office of Information Technology Services has initiated a Statewide Security Assessment Project. Details of the Security Assessment Project, including a description of the overall process, tasks, and roles and responsibilities are contained in the document entitled “Requirements - Statewide Security Assessment Project”.

The purpose of this document is to provide additional guidance and direction to State agencies to ensure that they are properly prepared to support the assessment effort. To that end, this document covers the following aspects of the security assessment project in detail:

- Security assessment scope and focus areas
- Agency resource requirements
- Documentation requirements
- Interview and scheduling guidance
- Contact information

2.0 Security Assessment Scope

The "depth" or level of detail that a security assessment goes into can, in general, be described by the following four increasing levels of assessment:

- Level 1 – Policy, Standards, and Procedures review
  - Essentially a "paper" review of policies, standards, and procedures
- Level 2 - "Eyes-on" Security Review
  - Reconciliation of security policies vs. deployment. Typically involves a certain level of spot-checking of key systems to verify compliance with standards
- Level 3 - "Hands-on" Security Review
  - Involves a detailed review of asset configurations
- Level 4 - Vulnerability Assessment
  - Involves a series of sanctioned attacks designed to probe system weaknesses

The State's Security Assessment Project will focus on the first two levels – Policy Standards and Guidelines Review and "Eyes-on Security" Review. The assessment Project is not intended to delve into either Level 3, which essentially represents a complete security audit, or Level 4 assessment activities.

In terms of "breadth" or extent, the assessment is expected to touch upon nearly every area of technology utilization, ranging from mainframe applications to cellular phone policies. It is recognized that not every agency employs every form of technology. However, for each technology area utilized by a given agency, the security assessment teams will assess agency security as it relates to the following ten topics as delineated in the ISO 17799 Security Standard:

1. Security policy
2. Organizational security
3. Asset classification and Control
4. Personnel
5. Physical security
6. Operations

7A. Access Control Administration
7B. Access Technology

8. Applications
9. Business Impact – Continuity
10. Compliance

Definitions for each of the above topics are included in Appendix A of this document.

Not every technology area will require a review against all ten topics listed above. For instance, agency intrusion detection policies are unlikely to require review for Physical Security. Appendix A of the project Requirements document contains a matrix that identifies which areas of focus apply to specific technologies. Agencies are requested to carefully review that information in preparation for their assessment.

3.0 Resource Requirements

As noted in the Requirements document, the State does not have sufficient time or resources to allow any agency assessment to fall behind schedule or run over budget. It is therefore imperative that agencies are properly prepared to support their security assessment. In order to ensure that agencies are prepared, the Project Management Office (PMO) has requested that agencies dedicated the appropriate resources to the assessment effort, including:

Assessment Liaison

The PMO requires that each agency identify an individual as their Assessment Liaison. Consistent with State statute, the agency's designated Security Liaison should perform the duties of Assessment Liaison. The Assessment Liaison will act as the primary point of contact for the security assessment and shall be responsible for agency preparation and cooperation. The Assessment Liaison shall track assessment progress from an agency perspective and shall ensure that agency resources are responsive to assessment support requirements. It is expected that the Assessment Liaison will participate in many of the assessment interviews and that the Liaison will generally be dedicated full-time to the assessment effort for the duration of data collection and diligence activities.

Assessment Coordinator

In most medium and large agencies, an Assessment Coordinator should be appointed to supplement the Assessment Liaison. The Assessment Coordinator will help to schedule interviews, collect the required documentation, and act as a second point of contact should the Assessment Liaison be unavailable. It is expected that Assessment Coordinator will be available during working hours, and that assessment support work will demand approximately 50 percent of the Coordinator's time during the preparation and data collection tasks.

In addition to the Assessment Liaison and Assessment Coordinator, the agency is requested to dedicate whatever additional resources are required to support a successful assessment. For instance, agencies are highly encouraged to ensure that appropriate representatives of senior management participate in key activities, including the Assessment Kick-Off Meeting and Agency Assessment Debrief Meetings described in the Requirements document. Also, agencies are encouraged to have a member of senior management issue a memorandum to agency personnel that restates the importance of the overall security assessment effort and reiterates senior management's dedication to supporting and cooperating with the effort.

4.0 Agency Documentation Requirements

The foundation for an accurate and meaningful security assessment is complete and accurate data collection. Best practices dictate that if an assessment team is unable to review certain data or documentation, the assessment team must assume that such documentation or data does not exist and must grade the assessment accordingly. It is, therefore, in the best interest of agencies to ensure that the assessment team is provided with complete and accurate data and documentation. Given the breadth and depth of assessment effort, data collection is an important and potentially sizeable task and agencies are highly encouraged to begin collecting relevant data and documentation well in advance of their assessment kick-off date.

In order to ensure that vendors are prepared and equipped with an understanding of the agency prior to commencing the interview and due diligence process, the agency must provide select information in advance of the assessment effort. Thus, five-days prior to the scheduled assessment kick-off date, each agency is required to submit the following documentation to the PMO:

- Completed Contact Information List
- Completed Interview Schedule
- Completed Agency Preparation Survey
- Organizational overview, vision/mission statements, etc.
- Organization chart at the division/office level
- Organization chart of technology support groups at the position level
  - List of personnel with security specific technology related duties
- Agency security policies, standards, procedures and guidelines, including, but not limited to:
  - Security Handbook/brochures/URLS for user community
  - Classified Information Handling Policy
  - Portable equipment / configuration policy
  - Email policy
- Critical Applications List
- List of Security Regulations Agency must comply with, including:
  - Legislation – State and Federal
  - Regulations required by Agency
- List of third party/outsourcing technology vendors (web hosting service providers, help desk, etc.) and their responsibilities
- Agency Documentation List

The last item noted above, the Agency Documentation List, is a key tool that will be used to register all agency documentation reviewed by vendor personnel and to record documentation disposition at project completion. Initially, the Agency shall record on the Documentation List a list of documentation that has been collected by the agency or is known to exist and that will be provided during the interview and due diligence process. The agency shall forward the Documentation List and the previously enumerated documents to the PMO five days in advance of the assessment. The PMO shall review and then turn over these materials to the assigned vendor, which shall then be responsible for maintaining the Agency Documentation List.

The following additional documents do not need to be submitted in advance, but will be handed to and reviewed by the vendor conducting the security assessment during the interview process. The following are examples of documents that the agency must provide to the security assessment vendor to review, if available:

- Network diagrams
- List of security tools available within agency
- Remote access configuration documentation
- Firewall configuration if maintained by agency
- Mobile/telecommuter configuration/policy
- Mainframe and midrange configuration documentation
- Applications access schema (ACL strategy or equivalent)
- Security infrastructure inventory (virus, firewall, etc)
- Operating systems, software infrastructure, middle-ware, etc.
- Web hosting and access services configuration documentation
- Desktop/laptop configuration information (standard image list, etc.)
- Hardware documentation including -model info (end user devices – PDAs, Laptops, Desktops, etc)
- Business continuity/disaster recovery (D/R) plan (2 copies on CD-ROM)
  - Identify D/R sites and/or vendors under contact
  - Location of D/R recovery files (site)
  - Recent test conducted and results
- Copy of recent Business Impact Analysis (BIA)/Risk Assessment
- Security headcount and budget
- Recent management reports including security metrics

- Job descriptions for any positions with information technology security responsibilities
- List of Security Training conducted at the agency level in the past year
- Third party information services contracts (e.g. Managed Security Services) with Service Level Agreements (SLAs)
- Additional information as may be requested by the vendor

Although vendors shall be responsible for proper disposition of all State materials upon completion of the project, agencies are responsible for proper classification of all information provided to vendors. Agencies are reminded that all confidential documentation must be appropriately marked per the requirements of G.S. §132-6.1(c) – i.e., stamped at the bottom with the phrase “CONFIDENTIAL per G.S. §132-6.1(c)”. Agencies are again encouraged to begin their data and documentation collection information at the earliest possible date.

5.0 Interview and Scheduling Guidance

Experience has shown that the ultimate success of a complex multi-faceted security assessment is highly dependent upon gaining access to the right individuals and the right information. To that end, the assessment teams will be conducting an extensive interview process to supplement and complement the review of available background materials. In order to maximize the value of the interview process, the following guidance is provided.

Interviews will typically run from sixty minutes to two hours in duration. The length of each interview will depend largely upon the volume of information that must be communicated. Correspondingly, some interviews, for instance with Human Resources to review background check policies, may be require only thirty minutes, while others, for instance with the WAN support group, may require up to three hours. As this varies widely by agency and function, the Assessment Coordination or Liaison should seek input from personnel identified by the agency for interviews (the interviewees) as to how long a given interview should be scheduled to last.

The following list provides general guidance as to who should be interviewed. Because the titles and positional responsibilities vary by agency, this list is not intended to be all-inclusive. In scheduling interviews, the agency must ultimately be guided by the dictum that all personnel with security responsibilities must be interviewed.

- Agency CIO
- Agency Security Liaison
- Technical Services Manager (and staff)
- Resource Access Control Manager
- System Security Administrator
- Applications Development Manager
- Applications Maintenance Manager
- Database Administrator
- Help Desk Manager
- Desktop and Desktop Applications Manager
- WAN Administrator
- LAN Administrator
- Human Resources
- Technology Procurement

Interviews should be arranged with individuals or for small groups (typically less than five interviewees) that share common security or technology management responsibilities. Although the interviews are most effective when the number of participants is held to a minimum, appropriate staff should attend as necessary to provide complete and accurate answers. In order to make the most effective use of the limited interview time available interviewees should be prepared to answer the questions listed below in addition to role- and technology-specific questions:

- *Briefly* describe the role of your organization or group. Please provide a brief overview of your organization including the number of employees, locations, etc.
- For what technologies is your organization responsible? What are your organization's specific security roles and responsibilities?
- Provide an overview of the security policies, standards and procedures that apply to your areas of responsibility.
- What security gaps have been previously identified? What mitigation efforts are on-going or planned to address those gaps?
- What constraints have limited your agency's ability to place more effective security measures in place?

To the extent practical, interviews should be scheduled to occur at a common location for the duration of the interview process. Sufficient time should be allowed between interviews to allow for interviews that run slightly long (typically 15 minutes is acceptable). To maximize the value of the interview process, all interviews should be conducted during a contiguous period starting immediately after the assessment kick-off meeting. For key stakeholders who are unable to participate during the scheduled interview process, the vendor will conduct a limited number of telephonic "make-up" interviews.

Agencies should note that more than one interview track might be required, as vendors may desire to perform several interviews in parallel. The Project Management Office will notify affected agencies in advance if such a requirement pertains. Conversely, if an agency believes that the assessment team must perform an interview outside of the Raleigh area, the agency should inform the PMO immediately. Due to limited travel budget, most of these interviews will have to be conducted telephonically.

As noted in Section 4, the Assessment Liaison must forward the following to the PMO at least five days in advance of the assessment start date.

- Completed Contact Information List
- Completed Interview Schedule

Both of these templates will be provided in an electronic format under separate cover for agency use. In short, these tools are intended to provide the assessment team with the necessary information to collect appropriate data and documentation. Once the PMO has reviewed the submitted information, it shall be turned-over to the assigned vendor along with all of the documentation provided by the agency. The vendor shall then coordinate any modifications or changes to the interview schedule directly with the agency.

6.0 Contact Information

Project Management Office

E-mail: security.pmo@ncmail.net
POC: Chris Turpin
Phone: (919) 981-2549

Appendix A – ISO 17799 Standard: Definitions

Security Policy

Security Policy control addresses management support, commitment, and direction in accomplishing information security goals, including:

- Information Security Policy document – a set of implementation-independent, conceptual information security policy statements governing the security goals of the organization. This document, along with a hierarchy of standards, guidelines, and procedures, helps implement and enforce policy statements.
- Ownership and review – Ongoing management commitment to information security is established by assigning ownership and review schedules for the Information Security Policy document.

Organizational Security

Organizational Security control addresses the need for a management framework that creates, sustains, and manages the security infrastructure, including:

- Management Information Security Forum – provides a multi-disciplinary committee chartered to discuss and disseminate information security issues throughout the organization.
- Information System Security Officer (ISSO) – acts as a central point of contact for information security issues, direction, and decisions.
- Information Security responsibilities – individual information security responsibilities are unambiguously allocated and detailed within job descriptions.
- Authorization processes – ensures that security considerations are evaluated and approvals obtained for new and modified information processing systems.
- Specialist information – maintains relationships with independent specialists to allow access to expertise not available within the organization.
- Organizational cooperation – maintains relationships with both information-sharing partners and local law-enforcement authorities.
- Independent review – mechanisms to allow independent review of security effectiveness.
- Third-party access – mechanisms to govern third-party interaction within the organization based on business requirements.
- Outsourcing – organizational outsourcing arrangements should have clear contractual security requirements.

Asset Classification and Control

Asset Classification and Control addresses the ability of the security infrastructure to protect organizational assets, including:

- Accountability and inventory: mechanisms to maintain an accurate inventory of assets, and establish ownership and stewardship of all assets.
- Classification – mechanisms to classify assets based on business impact.
- Labeling – labeling standards unambiguously brand assets to their classification.
- Handling – handling standards including introduction, transfer, removal, and disposal of all assets are based on asset classification.

Personnel Security

Personnel Security control addresses an organization's ability to mitigate risk inherent in human interactions, including:

- Personnel screening – policies within local legal and cultural frameworks ascertain the qualification and suitability of all personnel with access to organizational assets. This framework may be based on job descriptions and/or asset classification.
- Security responsibilities – personnel should be clearly informed of their information security responsibilities, including codes of conduct and non-disclosure agreements.
- Terms and conditions of employment – personnel should be clearly informed of their information security responsibilities as a condition of employment.
- Training – a mandatory information security awareness training program is conducted for all employees, including new hires and established employees.
- Recourse – a formal process to deal with violation of information security policies.

Physical and Environmental Security

Physical and Environmental Security control addresses risk inherent to organizational premises, including:

- Location – organizational premises should be analyzed for environmental hazards.
- Physical security perimeter – the premises security perimeter should be clearly defined and physically sound. A given premises may have multiple zones based on classification level or other organizational requirements.
- Access control – breaches in the physical security perimeter should have appropriate entry/exit controls commensurate with their classification level.
- Equipment – equipment should be sited within the premises to ensure physical and environmental integrity and availability.

- Asset transfer – mechanisms to track entry and exit of assets through the security perimeter.
- General – policies and standards, such as utilization of shredding equipment, secure storage, and "clean desk" principles, should exist to govern operational security within the workspace.

Communications and Operations Management

Communication and Operations Management control addresses an organization's ability to ensure correct and secure operation of its assets, including:
Operational procedures – comprehensive set of procedures, in support of organizational standards and policies.

- Change control – process to manage change and configuration control, including change management of the Information Security Management System.
- Incident management – mechanism to ensure timely and effective response to any security incidents.
- Segregation of duties – segregation and rotation of duties minimize the potential for collusion and uncontrolled exposure.
- Capacity planning – mechanism to monitor and project organizational capacity to ensure uninterrupted availability.
- System acceptance – methodology to evaluate system changes to ensure continued confidentiality, integrity, and availability.
- Malicious code - controls to mitigate risk from introduction of malicious code.
- Housekeeping – policies, standards, guidelines, and procedures to address routine housekeeping activities such as backup schedules and logging.
- Network management - controls to govern the secure operation of the networking infrastructure.
- Media handling – controls to govern secure handling and disposal of information storage media and documentation.
- Information exchange – controls to govern information exchange including end user agreements, user agreements, and information transport mechanisms.

Access Control

Access Control addresses an organization's ability to control access to assets based on business and security requirements, including:

- Business requirements – policy controlling access to organizational assets based on business requirements and "need to know."
- User management – mechanisms to:
  - Register and deregister users

- Control and review access and privileges
- Manage passwords

- User responsibilities – informing users of their access control responsibilities, including password stewardship and unattended equipment.
- Network access control – policy on usage of network services, including mechanisms (when appropriate) to:
  - Authenticate nodes
  - Authenticate external users
  - Define routing
  - Control network device security
  - Maintain network segregation or segmentation
  - Control network connections
  - Maintain the security of network services
- Host access control – mechanisms (when appropriate) to:
  - Automatically identify terminals
  - Securely log-on
  - Authenticate users
  - Manage passwords
  - Secure system utilities
  - Furnish user duress capability, such as “panic buttons”
  - Enable terminal, user, or connection timeouts
- Application access control – limits access to applications based on user or application authorization levels.
- Access monitoring – mechanisms to monitor system access and system use to detect unauthorized activities.
- Mobile computing – policies and standards to address asset protection, secure access, and user responsibilities.

System Development and Maintenance

System Development and Maintenance control addresses an organization’s ability to ensure that appropriate information system security controls are both incorporated and maintained, including:

- System security requirements – incorporates information security considerations in the specifications of any system development or procurement.

- Application security requirements – incorporates information security considerations in the specification of any application development or procurement.
- Cryptography – policies, standards, and procedures governing the usage and maintenance of cryptographic controls.
- System Integrity – mechanisms to control access to, and verify integrity of, operational software and data, including a process to track, evaluate, and incorporate asset upgrades and patches.
- Development security – integrates change control and technical reviews into development process.

Business Continuity Management

Business Continuity Management control addresses an organization's ability to counteract interruptions to normal operations, including:

- Business continuity planning – business continuity strategy based on a business impact analysis.
- Business continuity testing – testing and documentation of business continuity strategy.

Business continuity maintenance – identifies ownership of business continuity strategy as well as ongoing re-assessment and maintenance.

Compliance

Compliance control addresses an organization's ability to remain in compliance with regulatory, statutory, contractual, and security requirements, including:

- Legal requirements – awareness of:
  - Relevant legislation
  - Intellectual property rights
  - Safeguarding of organizational records
  - Data privacy
  - Prevention of misuse
  - Regulation of cryptography
  - Collection of evidence
- Technical requirements – mechanism to verify execution of security policies and implementations.
- System audits – auditing controls to maximize effectiveness, minimize disruption, and protect audit tools.

(Adapted from *Information Security Management: Understanding ISO 17799*, Lucent, 2001)